SSK Initiated by Third Party and Superposition Submissions

Abdulbast Abushgra, Advisor: Pro. Khaled Elleithy
Computer Science & Engineering Department
University of Bridgeport, Bridgeport, CT

FRD 2017

Introduction:

The Quantum Key Distribution **QKD** Protocol is a technical tool that helps to create a shared secret key (**SSK**) between communicated users. Moreover, to guarantee any connection over the internet, users should share an encrypted information as well as a decrypted cipher-text by a secret key. Furthermore, the QKD is a mechanism that creates a secret key into a secure mode. This poster shows an improvement of QKD protocol that is created by a connection with a trusted third party as well as the sender and receiver.

Initiating an EPR Connection:

1. The connection starts between the sender (*A*) and a third party (*C*).
2. *A* just prepares the plaintext that wants to share with the receiver (*B*).
3. The communication will be through a classical channel (*Internet, phone*).
4. The *C* will prepare the plaintext into a matrix (*DM*).

$$Bit[1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1] \approx \begin{cases} |0\rangle \\ |1\rangle \end{cases} \xrightarrow{EPR} preparations$$

5. The *C* submits an EPR string in two channels: first channel is for the sender *A*, and the second channel is for the receiver *B*.

$$plaintext = \begin{Bmatrix} \omega & \mu & \mu \\ \varphi & \omega & \mu \\ \varphi & \varphi & \omega \end{Bmatrix},$$

where φ is the plaintext that is converted to entangled states, μ is the random states that *C* will randomly set, and ω is parity cells for decoy states.

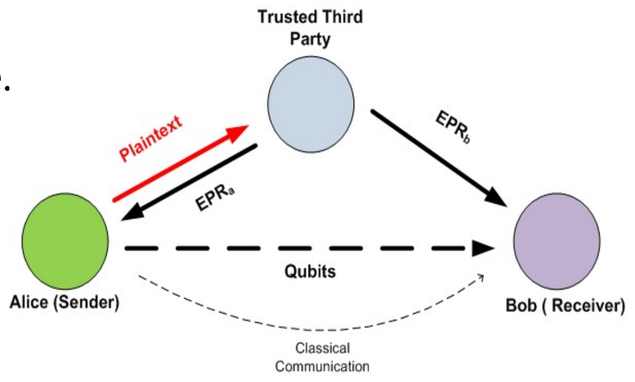
Approval Confirmation:

- Each side of the communication (*A & B*) will receive data into EPR channel, where each side has a converted information compared to the other side.

$$|\Phi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}), \qquad |\Psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}).$$

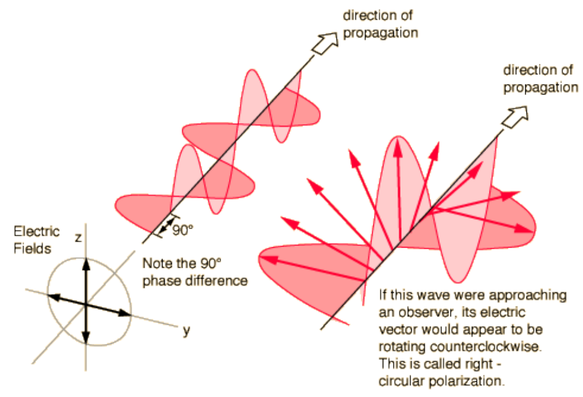
- The submitted data is highly classified to be a secure.
- There is no interruption without alteration.
- Flipped states will impact a different measurement.

$$|\varphi_{AB}\rangle \begin{cases} |0\rangle \\ |1\rangle \end{cases}$$
$$if\ A == 1, then\ B = 0$$



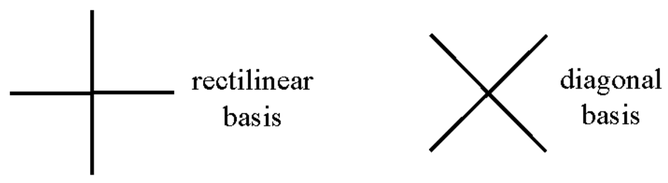
QUBIT Submissions:

- The submission through the Quantum channel (*in superposition*) will be limited between the *A* and *B*.



$$|\varphi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle \pm \beta|1\rangle),$$

- Two bases for measurements:



- Four states:

$$(|0\rangle, |90\rangle, |45\rangle, |135\rangle)$$

System Requirements:

To process this protocol, there are some needed requirements that should available:

- Entanglement Channel.

- Quantum Gates:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$Y|0\rangle = i|1\rangle, \quad Y|1\rangle = -i|0\rangle$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle$

Shared Secret Key:

The **SSK** is the final result of the quantum key distribution protocol, where a string of qubits will be shared in a secure mode.

Example:
String of qubits
$[|1\rangle, |1\rangle, |0\rangle, |1\rangle, |0\rangle, |0\rangle, |1\rangle, |1\rangle]$,

String of bits
[1, 1, 0, 1, 0, 0, 1, 1].

Finally, it should be used one time.

References:

[1] A. Abushgra and K. M. Elleithy, "Simultaneous Initiating EPR and Quantum Channel by AK15 Protocol," 2016.
[2] A. Abushgra and K. Elleithy, "Initiated decoy states in quantum key distribution protocol by 3 ways channel," in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, 2015, pp. 1-5.
[3] A. Abushgra and K. Elleithy, "Security of Quantum Key Distribution," 2015.
[4] Khaled. Elleithy. Abdulbast Abushgra, "Indexing Qubits Based on Matrix Processing By QKDP's," Journal Of Theoretical Physics & Cryptography, vol. 12, pp. 1-5, 2016.